Carnegie Mellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Staying informed

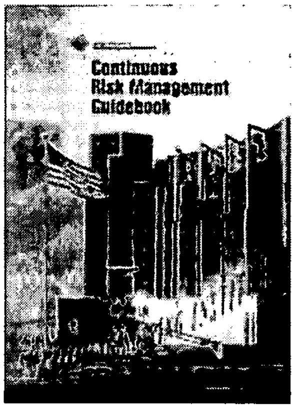
About the SEI | Management | Engineering | Acquisition | Work with Us | Products and Services | Publications

PUBLICATIONS

- Publications Home
- Lists of SEI Reports
- Recent Reports
- Annual Report
- Books
- news@sei
- File Formats
- Paper Copies of SEI Reports
- FAQ

Continuous Risk Management Guidebook

Are your development projects over budget and behind schedule because of unexpected and unplanned-for problems?



Authors

Richard L. Murphy
Christopher J. Alberts
Ray C. Williams
Ronald P. Higuera
Audrey J. Dorofee
Julie A. Walker

Who should read this publication?

-Professionals directly involved in software-intensive projects (program managers, lead engineers, software engineers, etc.)

-Professionals from other disciplines (e.g., quality assurance, hardware engineering, testing) involved in software-intensive projects.

-Sponsors, change agents, technology transition agents, and software engineering process group members in organizations that want to improve.

Description

The *Continuous Risk Management Guidebook* describes the underlying principles, concepts, and functions of risk management and provides guidance on how to implement it as a continuous practice in your projects and organization. Risk management can be used to continuously assess what can go wrong in projects (i.e., what the risks are), determine which of these risks are most important, and implement strategies to deal with these risks. The guidebook is based on proven practices confirmed through research, field testing, and direct work with clients.

The *Continuous Risk Management Guidebook* was developed to help a project or organization establish continuous risk management as a routine practice and then continue to improve this process. It is organized so that different users can read different parts of the book and get different benefits. For example, technical managers and lead engineers can read the book to learn how to build a risk management process that is tailored to their specific project or organization; software engineers can use it to understand how to perform the risk management methods and use the tools described in the guidebook; and change agents (such as members of software engineering process groups) can read it to understand why continuous risk management should be used and how to get projects to tailor it and start using it. In addition, all users of this guidebook will gain a greater understanding of continuous risk management.

The authors describe both what continuous risk management is and how to implement it. They explain the concepts, principles, and functions of continuous risk management in detail and provide a view of what risk management could look like when implemented within a project. It then shows how an organization might tailor continuous risk management to fit in its specific environment, provides methods and tools that can be used to perform continuous risk management, and presents a roadmap to help organizations install a continuous risk management process. Although this guidebook deals primarily with performing continuous risk management in a software development environment, it can easily address systems, hardware, and other domains.

The information in this guidebook will help an organization address the following questions:

- What is continuous risk management and why would I want to use it?
- What does continuous risk management look like when implemented within a typical project?
- What risk information should be collected?
- How would a project get started and install continuous risk management?
- What do you need to put in place for a successful risk management program?
- What methods and tools can be used to perform continuous risk management?

Prerequisites

Successful users typically have

- development experience with software-intensive systems
- commitment to change and improvement

Sample Pages

Sample pages of the guidebook are available in portable document format (PDF).

Author Team

The authors have more than 90 years of software development experience in defense, aeronautics, robotics, commercial, steel, and nuclear industries, including more than 25 years in the field of risk management. In the last six years, they and other members of the Software Engineering Institute (SEI) Risk Program have worked with more than 50 programs from the Department of Defense, civil agencies, and industry. The programs have ranged from large-scale aerospace programs to small, turnkey projects. These efforts have ranged from stand-alone risk assessments to broad-based, organization-wide adaptation and implementation of risk management practices. This guidebook codifies the best practices in risk management.

top row: Richard L. Murphy, Christopher J. Alberts,
Ray C. Williams, and Ronald P. Higuera
bottom row: Audrey J. Dorofee and Julie A. Walker

Related SEI Products and Services

Related Courses
Continuous Risk Management Course

Related Publication
Software Acquisition Capability Maturity Model®

Related Services
Team Risk Management Service
Continuous Risk Management Service
Software Risk Evaluation Service

Software Risk Evaluation is a service that helps projects to establish an initial baseline set of risks and mitigation plans-one of the key first steps for putting risk management in place. Team Risk Management extends Continuous Risk Management to include all partners in a program (e.g., customer, supplier, subcontractors, etc.).

Availability

This guidebook will be included in the Continuous Risk Management Training course and Continuous Risk Management consulting services, at no additional cost.

Order

Download the order form, complete it, and mail or FAX it to:

Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Phone: 412-268-5800
FAX: 412-268-5758
E-mail: customer-relations@sei.cmu.edu

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html
Last Modified: 14 January 2005

CarnegieMellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Acquire
Improving acquisition practices.
Support

About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

ACQUISITION

- ● Main page
- ○ Frequently Asked Questions
- ○ Overview
- ○ Paradigm
- ○ Principles
- ○ Products
- ○ Team Risk Management Overview
- ○ Bibliography
- ○ Reports

Risk Management

Background | SEI Risk Statement | Risk Examples
Software Risk Evaluation | Continuous Risk Management Guidebook
Risk Process Check | For More Information

Background

The term **risk management** is applied in a number of diverse disciplines. People in the fields of statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory, to name a few, have been addressing the field of risk management.

Kloman summarized the meaning of risk management in the context of a number of different disciplines in an article for *Risk Analysis*:

"What is risk management? To many social analysts, politicians, and academics it is the management of environmental and nuclear risks, those technology-generated macro-risks that appear to threaten our existence. To bankers and financial officers it is the sophisticated use of such techniques as currency hedging and interest rate swaps. To insurance buyers and sellers it is coordination of insurable risks and the reduction of insurance costs. To hospital administrators it may mean 'quality assurance.' To safety professionals it is reducing accidents and injuries."

Kloman Paraphrase of Rowe
Risk management is a discipline for living with the possibility that future events may cause adverse effects.

Return to top ▲

SEI Risk Statement

For a risk to be understandable, it must be expressed clearly. Such a statement must include

- a description of the current conditions that may lead to the loss
- a description of the loss

Risk Example

A company has introduced object-oriented (OO) technology into its organization by selecting a well-defined project "X" with hard schedule constraints to pilot the use of the technology. Although many "X" project personnel were familiar with the OO concept, it had not been part of their development process, and they have had very little experience and training in the technology's application. It is taking project personnel longer than expected to climb the learning curve. Some personnel are concerned, for example, that the modules implemented to date might be too inefficient to satisfy project "X" performance requirements.

The risk is: Given the lack of OO technology experience and training, there is a possibility that the product will not meet performance or functionality requirements within the defined schedule.

Non-Risk Example

Another company is developing a flight control system. During system integration testing the flight control system becomes unstable because processing of the control function is not quick enough during a specific maneuver sequence.

The instability of the system is not a risk since the event is a certainty - it is a problem.

Continuous Risk Management Example

When using Continuous Risk Management, risks are assessed continuously and used for decision-making in all phases of a project. Risks are carried forward and dealt with until they are resolved or they turn into problems and are handled as such.

Non-Continuous Risk Management Example

In some projects, risks are assessed only once during initial project planning. Major risks are identified and mitigated, but risks are never explicitly looked at again.

This is not an example of Continuous Risk Management because risks are not continuously assessed and new risks are not continuously identified.

Return to top ▲

Software Risk Evaluation

The SEI Software Risk Evaluation (SRE) Service is a diagnostic and decision-making tool that enables the identification, analysis, tracking, mitigation, and communication of risks in software-intensive programs. An SRE is used to identify and categorize specific program risks emanating from product, process, management, resources, and constraints. The program's own personnel participate in the identification, analysis, and mitigation of risks facing their own development effort.

An SRE provides a program manager with a mechanism to anticipate and address program risks. The SRE introduces a set of activities that, when initiated, begin the process of managing risk. These activities can be integrated with existing methods and tools to enhance program management practices.

For more information, see Software Risk Evaluation Service Web page.

Return to top ▲

Risk Process Check

A Risk Process Check is the SEI's most recently developed risk management service. It is combination of tutorial, survey instrument, interviews, and feedback session conducted on-site to determine how effective the project or program's risk management process is. It is based on the SEI's Seven Principles of Risk Management, and, being principle-based rather than model-based, it can evaluate any risk management process, whether it follows the guidelines of the SEI's Continuous Risk Management course or some completely different model.

The Risk Process Check has been used on one major DoD program (DoD program office, prime contractor, and two subcontractors to the prime) and two contractor organizations to a non-DoD government agency. There are many areas of opportunity to refine and further define this service with the SEI.

Continuous Risk Management Guidebook

The Continuous Risk Management Guidebook was written with professionals in mind who are directly involved in software-intensive projects (program managers, lead engineers, software engineers, etc.). It may also be of interest to professionals from other disciplines (e.g., quality assurance, hardware engineering, testing) involved in software-intensive projects, and sponsors, change agents, technology transition agents, and software engineering process group members in organizations that want to improve.

The *Continuous Risk Management Guidebook* describes the underlying principles, concepts, and functions of risk management and provides guidance on how to implement it as a continuous practice in your projects and organization. Risk management can be used to continuously assess what can go wrong in projects (i.e., what the risks are), determine which of these risks are most important, and implement strategies to deal with these risks. The guidebook is based on proven practices confirmed through research, field testing, and direct work with clients.

The *Continuous Risk Management Guidebook* was developed to help a project or organization establish continuous risk management as a routine practice and then continue to improve this process. It is organized so that different users can read different parts of the book and get different benefits. For example, technical managers and lead engineers can read the book to learn how to build a risk management process that is tailored to their specific project or organization; software engineers can use it to understand how to perform the risk management methods and use the tools described in the guidebook; and change agents (such as members of software engineering process groups) can read it to understand why continuous risk management should be used and how to get projects to tailor it and start using it. In addition, all users of this guidebook will gain a greater understanding of continuous risk management.

Although the Guidebook deals primarily with performing continuous risk management in a software development environment, it can easily address systems, hardware, and other domains.

For more detailed information, visit the CRM Guidebook Web page.

Return to top ▲

For More Information

See A Taxonomy of Operational Risks (PDF), a presentation by Brian Gallagher at the 8th Annual Systems Engineering Conference, October 24-27, 2005

Send comments or questions to:
Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Forbes Avenue
Pittsburgh, PA 15213-3890
Phone: 412-268-5800
E-mail: customer-relations@sei.cmu.edu

Return to top ▲

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/risk/main.html
Last Modified: 3 November 2005

CarnegieMellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Acquire Improving acquisition practices Support

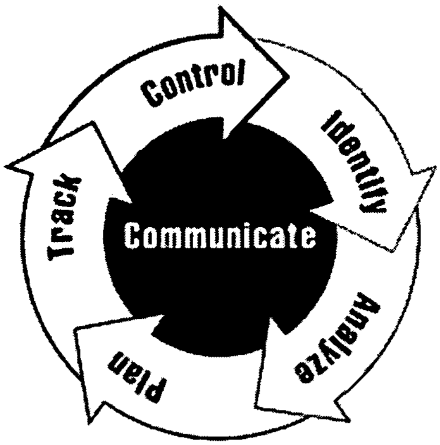
About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

ACQUISITION

- ○ Main page
- ○ Frequently Asked Questions
- ○ Overview
- ● Paradigm
- ○ Principles
- ○ Products
- ○ Team Risk Management Overview
- ○ Bibliography
- ○ Reports

Risk Management Paradigm

The SEI Risk Management Paradigm is depicted below. The paradigm illustrates a set of functions that are identified as continuous activities throughout the life cycle of a project.



Functions of Continuous Risk Management

The functions of Continuous Risk Management are introduced below. Each risk nominally goes through these functions sequentially, but the activity occurs continuously, concurrently (e.g., risks are tracked in parallel while new risks are identified and analyzed), and iteratively (e.g., the mitigation plan for one risk may yield another risk) throughout the project life cycle.

Function	Description
Identify	Search for and locate risks before they become problems.
Analyze	Transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks.
Plan	Translate risk information into decisions and actions (both present and future) and implement those actions.
Track	Monitor risk indicators and mitigation actions.
Control	Correct for deviations from the risk mitigation plans.
Communicate	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks.

Note: Communication happens throughout all the functions of risk management.

For More Information

Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Forbes Avenue
Pittsburgh, PA 15213-3890
Phone: 412-268-5800

Send comments or questions to customer-relations@sei.cmu.edu

Return to top ▲ | Risk Management main page

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/risk/paradigm.html
Last Modified: 3 November 2005

CarnegieMellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Acquire
Improving acquisition practices
Support

About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

The Principles of Risk Management

ACQUISITION

- ○ Main page
- ○ Frequently Asked Questions
- ○ Overview
- ○ Paradigm
- ● Principles
- ○ Products
- ○ Team Risk Management Overview
- ○ Bibliography
- ○ Reports

These seven principles provide a framework to accomplish effective risk management. These principles are embodied within our risk management products and services which addresses the need to establish a baseline set of risks in a project or program (Software Risk Evaluation), the need to create and implement a continuous process for the effective management of risk (Continuous Risk Management), and the need to include all parts of the program (contractors, customers, etc.) in the joint management of risks (Team Risk Management).

Global perspective	• Viewing software development within the context of the larger systems-level definition, design, and development. • Recognizing both the potential value of opportunity and the potential impact of adverse effects.
Forward-looking view	• Thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes. • Managing project resources and activities while anticipating uncertainties.
Open communication	• Encouraging free-flowing information at and between all project levels. • Enabling formal, informal, and impromptu communication. • Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk).
Integrated management	• Making risk management an integral and vital part of project management. • Adapting risk management methods and tools to a project's infrastructure and culture.
Continuous process	• Sustaining constant vigilance. • Identifying and managing risks routinely through all phases of the project's life cycle.
Shared product vision	• Mutual product vision based on common purpose, shared ownership, and collective communication. • Focusing on results.
Teamwork	• Working cooperatively to achieve common goal.

	• Pooling talents, skills, and knowledge.

For More Information

Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Forbes Avenue
Pittsburgh, PA 15213-3890
Phone: 412-268-5800

Send comments or questions to customer-relations@sei.cmu.edu

Return to top ▲ | Risk Management main page

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/risk/principles.html
Last Modified: 3 November 2005

CarnegieMellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Acquire
Improving acquisition practices.
Support

About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

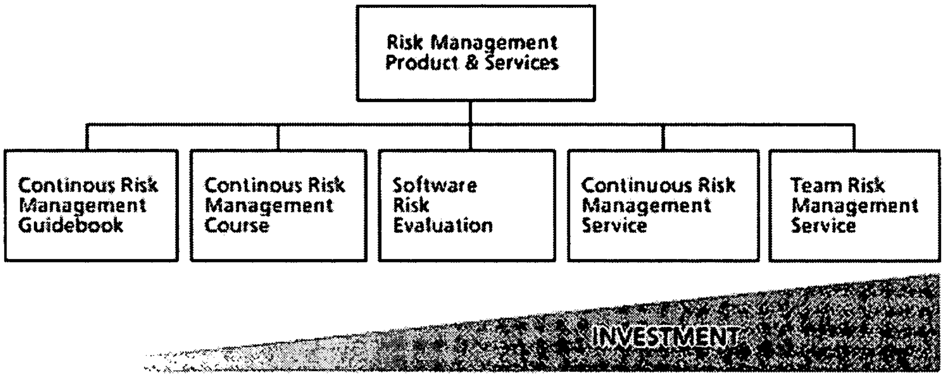
Risk Management Products and Services

ACQUISITION

- ○ Main page
- ○ Frequently Asked Questions
- ○ Overview
- ○ Paradigm
- ○ Principles
- ● Products
- ○ Team Risk Management Overview
- ○ Bibliography
- ○ Reports

Are your development projects over budget and behind schedule because of unexpected problems you didn't plan for? Do you leave work on Friday with everything under control and come in on Monday to a crisis? Do you feel as if there are problems lurking around every corner but you just can't see them clearly enough to avoid them?

The SEI risk management products and services can help you to gain control over the uncertainty in your projects to proactively manage rather than react to one crisis after another.


Risk Management Product & Services
Continous Risk Management Guidebook
Continous Risk Management Course
Software Risk Evaluation
Continuous Risk Management Service
Team Risk Management Service
INVESTMENT

I'm curious and I want to know more.
I have little knowledge about risk management in general or about the SEI risk management. I want to know what risk management is, the types of methods and tools that could be used, and how it all fits together.

Recommended: Risk Management Overview and Continuous Risk Management Guidebook.

My organization needs training. I want my project or personnel to know how to manage their risks.
My team needs hands-on practice and exercise to instill skills. I want to get an entire project up to speed rapidly.

Recommended: Continuous Risk Management Course (includes Continuous Risk Management Guidebook)

I need to know what my project's risks are now and what to do about them.
I need to get started immediately to find the project's risks and start mitigating them.

Recommended: Software Risk Evaluation

Recommended Follow-on: Continuous Risk Management Course or Continuous Risk Management Service

---

I need to get risk management up and running in my project.
I know what risk management is, and I want to do it on this project. We need to have methods and tools that will integrate into current project management practices, that will blend into what we do now.

Recommended: Continuous Risk Management Service

All organizations in this program need to manage their risks, not just the contractor.
We know what risk management is, and want all the organizations on this program to be jointly involved (e.g., customer and supplier, subcontractors, etc.). Everyone needs to work together to make this program a success.

Recommended: Team Risk Management Overview and Team Risk Management Service

Recommended Prerequisite: Continuous Risk Management Course or Continuous Risk Management Service

---

For More Information

Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Forbes Avenue
Pittsburgh, PA 15213-3890
Phone: 412-268-5800

Send comments or questions to customer-relations@sei.cmu.edu

Return to top ▲ | Risk Management main page

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/risk/risk.products.html
Last Modified: 3 November 2005

Software Risk Evaluation Service

Who might need this service?

Program/project managers and development teams seeking a disciplined approach to proactive program management

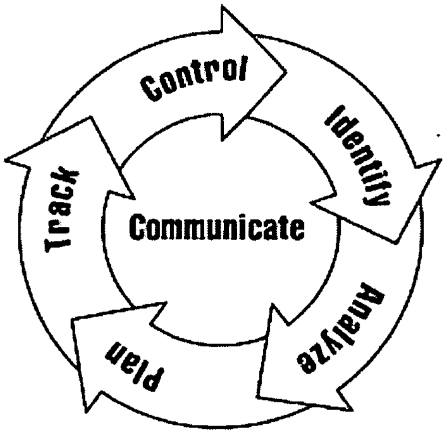
Are you concerned about the risks that threaten your program's success?

Do you want to anticipate and address today's risks before they become tomorrow's problems?

The SEI Software Risk Evaluation (SRE) Service is a diagnostic and decision-making tool that enables the identification, analysis, tracking, mitigation, and communication of risks in software-intensive programs. An SRE is used to identify and categorize specific program risks emanating from product, process, management, resources, and constraints. The program's own personnel participate in the identification, analysis, and mitigation of risks facing their own development effort.

An SRE provides a program manager with a mechanism to anticipate and address program risks. The SRE introduces a set of activities that, when initiated, begin the process of managing risk. These activities can be integrated with existing methods and tools to enhance program management practices. The SRE can be used for several purposes:

- diagnostic - Are the risks acceptable for starting a program?
- baselining - The SRE identifies a critical set of risks before they become problems so they can be managed on a continuous basis.
- preparing for a critical milestone
- "recovering from crisis" - The SRE provides a way to reset a baseline for a program.



An SRE is conducted by a trained SEI-program team. It carries out the activities of the SRE in the following phases:

- Contracting - SREs are performed only with the commitment of the executives in charge of the program and the direct involvement of the development staff.
- Risk Identification & Analysis (onsite)- The SRE team meets with program staff members (e.g. program manager, engineers, support personnel) to identify risks. Later, risks are analyzed and grouped into major risk areas.
- Interim Report - The SRE team constructs a risk area interrelationship digraph to be the basis for their recommendation of the areas to be addressed during Mitigation Strategy Planning, combines it with a summary of the results of Risk Identification & Analysis, and presents the recommendation and summary to the program manager. The program manager decides which risk areas are to be addressed.
- Mitigation Strategy Planning (onsite)- The SRE team helps program personnel construct a set of coordinated mitigation plans for the most important risk areas.
- Final Report and Closure - The SRE team writes a final report detailing the findings and plans.

The SEI can also provide post-evaluation support tailored to the client's specific needs and can help put a continuous risk management paradigm and ethos in place.

The SEI is the federal government's principal source of expertise on the state of the practice in software engineering. By implementing a Software Risk Evaluation, management improves its ability to assure success through the creation of a proactive risk management methodology.

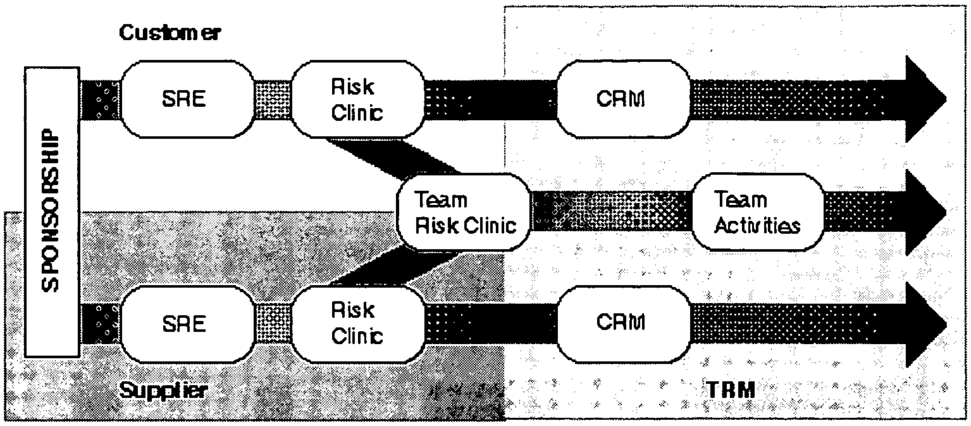
How does the Software Risk Evaluation fit in to other Risk products and services?

The Software Risk Evaluation (SRE) is a service that helps projects establish an initial baseline set of risks and mitigation plans -- one of the key first steps for putting risk management in place.

The Risk Clinic is the workshop that initiates the Continuous Risk Management (CRM) Service within an organization. The clinic can be used to tailor CRM to suit a client's specific needs and to implement it in one or more programs.

Continuous Risk Management (CRM) builds upon the results of the SRE and advances programs to managing risk on a continuing basis. It includes a number of methods to accomplish this task at the program level and to install a continuous risk management process at the organizational level.

The Team Risk Clinic is the workshop that initiates the Team Risk Management (TRM) Service. The clinic can be used to tailor TRM to suit the clients' specific needs and to implement it in all the partners in a program (e.g. customer, supplier, subcontractors, etc.).



Team Risk Management (TRM) extends CRM to include all partners in a program. TRM brings about joint management of risks in a collaborative fashion. The diagram above summarizes these relationships.

Developers
George Pandelios, Sandra Behrens, Ray Williams, William Wilson, Julie Walker, and Richard Murphy

The developers represent more than 50 years of combined systems and software development and risk management experience. The SRE is the product of many contributors and the culmination of numerous separate, proven techniques. However, without the fundamental contributions of those named below, the SRE would not exist today.

Frank J. Sisti, Sujoe Joseph, William G. Wood, F. Michael Dedolph, and Carol Ulrich developed and tested Version 1.0 of the Software Risk Evaluation. Marvin Carr, Suresh Konda, Carol Ulrich, Clay Walker, and Ira Monarch developed the SEI Software Risk Taxonomy. F. Michael Dedolph and Ray C. Williams adapted the Interrelationship Digraph technique for use in the SRE. Audrey Dorofee and Julie Walker contributed to the development of Mitigation Strategy Planning activities. Dick Murphy, Ray Williams, Julie Walker, and George Pandelios worked on the initial collection and harmonization of these various techniques into the V2 SRE. George Pandelios, Sandra Behrens, Dick Murphy, Ray Williams, and William Wilson operationally tested, modified, and packaged the software risk evaluation.

Related SEI Products and Services

Related Courses
Continuous Risk Management Course

Related Services
Continuous Risk Management Service
Team Risk Management

Related Publications
Continuous Risk Management Guidebook

For more information about the SEI and its products and services, contact

Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412-268-5800
FAX: 412-268-5758
E-mail: customer-relations@sei.cmu.edu

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/products/services/sw.risk.eval-service.html
Last Modified: 30 August 2005

Carnegie Mellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

Building your skills

PRODUCTS AND SERVICES

- Course Offerings
- Prices
- Locations and Travel Information
- Courses FAQ
- Registration
- Contact Information
- Credentials Program

Continuous Risk Management

Dates

2006 Dates
March 1-2, 2006 (SEI Pittsburgh, PA)
June 14-15, 2006 (SEI Pittsburgh, PA)
September 13-14, 2006 (SEI Pittsburgh, PA)

Prices (USD)

U.S.
Industry: $1100
Government: $880
Academic: $880

International
$2200

Course Registration
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-7388
FAX: 412 / 268-7401
E-mail: courseregistration@sei.cmu.edu

2006
REGISTER

This course may also be offered by arrangement at customer sites. E-mail course-info@sei.cmu.edu or call +1 412-268-7622 for details.

Course Description

This two-day course introduces project managers, lead engineers, software engineers, quality assurance staff, hardware engineers, and software engineering process group (e.g., EPG, SEPG) members to the concepts and application of continuous risk management. The course closely follows the risk management practices described in the *Continuous Risk Management Guidebook* and provides practical experience with methods and tools that aid participants in implementing these practices.

The course is composed of lectures, class discussions, and case study exercises. Participants work individually and in small groups to learn the skills and tools needed to implement continuous risk management. After attending, participants will be able to apply what they have learned to their organization's projects.

Audience · Prerequisites · Objectives · Logistics

AUDIENCE

- project managers, lead engineers, and software engineers involved in software-intensive projects
- those involved in software-intensive projects from related disciplines such as quality assurance, hardware engineering, and testing
- engineering process group (e.g., SEPG, EPG) members
- change agents and technology transition agents

PREREQUISITES

There are no prerequisites for this course.

TOPICS

- Risk Management - overview & background
- Identify - creating risk statements and context
- Analyze - evaluating, classifying, and prioritizing risk statements and risk areas
- Plan - creating mitigation strategies for risk statements and risk areas
- Track - collecting and presenting appropriate data on risk statements and risk plans
- Control - analyzing risk data and acting on it

OBJECTIVES

This course helps participants to

- understand and apply the concepts, principles, and tools of Continuous Risk Management
- develop basic risk management skills for each function of Continuous Risk Management
- understand basic concepts of tailoring Continuous Risk Management to a project
- be able to use the Continuous Risk Management Guidebook effectively as a reference

Course Materials

On the first day of the course, participants will receive the *Continuous Risk Management Guidebook*, a Software Risk Evaluation CD-ROM with risk identification interview videos, a course notebook, and a case study.

LOGISTICS

Class Schedule

This 2-day course meets at the following times:
Days 1-2, 8:30 a.m. - 5:00 p.m.

Hotel and Travel Information

Information about traveling to SEI offices in Pittsburgh, Pennsylvania and Arlington, Virginia is available on our Travel and Lodging Web pages.

Questions about this course?

Please see our Frequently Asked Questions Web page for answers to some of the more common inquiries about SEI Education and Training. If you need more information, contact us via e-mail at course-info@sei.cmu.edu or telephone at +1 412-268-7622.

Related Products and Services

Courses

Managing Technological Change
Introduction to CMMI, Continuous Representation
Introduction to CMMI, Staged Representation
Software Acquisition Survival Skills

Publications

Dorofee, Audrey, et. al. *Continuous Risk Management Guidebook*, Pittsburgh, PA: Carnegie Mellon University, 1996.

Williams, Ray, et. al. *Software Risk Evaluation Method Description & SRE*

Team Member's Notebook, Version 2.0 (CMU/SEI-99-TR-029), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 1999.

CMMI Product Development Team. *CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1 Continuous Representation* (CMU/SEI-2002-TR-011, ESC-TR-2002-011). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, November 2000.

CMMI Product Development Team. *CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1 Staged Representation* (CMU/SEI-2002-TR-012, ESC-TR-2002-012). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, November 2000.

Events
Software Engineering Process Group (SEPG) Conference
CMMI Technology Conference and Users Group
Australian Software Engineering Process Group (SEPG) Conference
European Software Engineering Process Group (SEPG) Conference

Services
Continuous Risk Management Service
Software Risk Evaluation
Team Risk Management

Course Registration

2006

REGISTER

^
TOP

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/products/courses/crm.course.html
Last Modified: 27 September 2005